8 June 1972

STAT [ ] NATIONAL SECURITY INFORMATION — CLASSIFICATION, DECLASSIFICATION AND ACCESS

PART I. INTRODUCTION

A. Executive Order 11652 — CIA Implementation. Executive Order 11652 and the implementing National Security Council Directive of May 17, 1972, regulate and control the protection and management of national security information and material and provide for access to such information. This regulation is the Agency implementation of those portions of the foregoing directives which impose requirements with respect to classifying, declassifying and managing, and concerning access to such information. [ ] is the implementation of the provisions of E.O. 11652 concerning storage. [ ] implements the provisions concerning transmission and destruction.

STAT STAT

B. Purposes — CIA Administration. The primary purpose of the Executive Order and the Directive obviously is to protect information involving national security. An equally important objective is to prevent the system for protecting such information from operating to prevent, unnecessarily or improperly, information from becoming

available to the public. To accomplish these objectives, the two directives require the classification of national security information, prohibit its overclassification or classification for improper reasons, and require prompt and orderly declassification when national security considerations permit such action. Physical protection of national security information is required, access to such information is limited, and effective measures to manage such information are required. Agency implementation and administration of the Order will seek to accomplish these objectives. The responsibility of the Director to protect intelligence sources and methods, as prescribed by the National Security Act of 1947, also will be implemented by CIA actions under the Order.

C. Effective Dates. The Executive Order and NSC Directive are effective June 1, 1972. This revision of [ ] shall become effective on 1972. STAT

D. Definitions. The following definitions are prescribed by E.O. 11652.

1. National Security Information. National security information is information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States.

2. Top Secret. Top Secret refers to that national security information or material which requires the highest degree of protection. The test for assigning Top Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

3. Secret. Secret refers to that national security information or material which requires a substantial degree of protection. The test for assigning Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

4. Confidential. Confidential refers to that national security information or material which requires protection. The test for assigning Confidential classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

PART II. CLASSIFYING INFORMATION — MARKING DOCUMENTS

A. Persons Authorized to Classify. The authority to classify information, prescribed below, may not be redelegated.

1. Top Secret. Information and material may be classified Top Secret only by the Director and by officials designated by the Director in writing, in accordance with the Executive Order.

2. Secret. Information and material may be classified Secret only by Top Secret classifiers and by officials authorized in writing by Top Secret classifiers.

3. Confidential. Information and material may be classified Confidential only by Top Secret and Secret classifiers and by officials authorized in writing by Top Secret and Secret classifiers.

B. Guidelines for the Exercise of Classification Authority. A determination shall be made with respect to each document originated by CIA as to which security classification category (Top Secret, Secret or Confidential), if any, is applicable to the document. If the originator of the document has been delegated classification authority under Section A of this PART which in his judgment is appropriate to the document, the determination shall be made by him. Otherwise, he shall forward the document to an official who possesses the requisite authority, who

thereupon shall determine the classification to be given the document. The classification decision shall be based on the definitions of security information (PART I, Section D) and the principles prescribed in the following paragraphs.

1. Presidential Restrictions. The Executive Order or the NSC Directive provides that:

(a) Top Secret classification authority shall be used with the "utmost restraint."

(b) Secret classification authority shall be "sparingly used."

(c) Both unnecessary classification and overclassification shall be avoided. Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security.

(d) If the classifier has any substantial doubt as to which security classification category is appropriate, or as to whether the material should be classified at all, he should designate the less restrictive treatment.

2. Statutory Responsibilities of CIA. By statute, the Director is "responsible for protecting intelligence sources and methods from unauthorized disclosure". Intelligence and intelligence sources and methods inherently involve a mosaic of information. Isolated and apparently unrelated items of information therefore could endanger or reveal intelligence sources and methods.

3. Superior Level Decisions Binding. Whenever a subject, program, operation or project has been classified by the Director, a Deputy Director or another official authorized to make that decision (including non-CIA officials), that decision controls the decisions of all other persons with respect to any documents of a substantive nature originated by them involving such matter. [redacted] ILLEGIB

4. Foreign Information. Classified information or material furnished to the United States by a foreign government or international organization shall be afforded a degree of protection equivalent to or greater than that required by the foreign classification marking. If there is no U. S. equivalent for the foreign marking, the foreign document should be marked with the next higher U. S. classification (e. g., [redacted] STAT

[redacted] STAT

5. Referenced Information. Material containing references to classified materials, which references do not reveal classified information, shall not be classified.

6. Physically-Connected Documents. Files, containers and other items which contain documents, files, products or substances shall be classified at least as high as that of the most highly classified component therein. When it is feasible to do so, documents of differing security classification should not be physically connected.

7. Restricted Data. Restricted Data (atomic energy information) and Formerly Restricted Data shall be classified, declassified and downgraded in conformity with the Atomic Energy Act.

C. Additional Classification Guidelines.

1. No Other Security Classification Categories Permitted. Except as expressly provided by statute, no security classification category other than Top Secret, Secret or Confidential shall be used to identify official information as requiring protection in the interest of national security.

2. Special Protective Measures May Be Imposed. With the prior specific approval of the Executive Director, special measures, including compartmentation systems, may be imposed with respect to access, distribution and protection of classified information and material,

including that which relates to communications intelligence, intelligence sources and methods, and cryptography. Special measures in existence on the effective date of the Order are not invalidated by the Order, the NSC Directive or this regulation, but continue in effect without reissuance or reapproval.

3. Reconsiderations of Classification Decision. If a recipient or holder of a classified document believes the document is classified at the wrong level or that the document should be subject to the General Declassification Schedule (see PART III, Section A, paragraph 1), he shall so recommend to the original classifier. The original classifier thereupon shall reconsider the classification and, if warranted, remove or change it.

4. Classifiers Accountable For Their Actions. Each employee possessing classification authority shall be held accountable for the propriety of the classifications attributed to him.

D. Marking Classified Documents.

1. Documents Generally. At the time of origination of a document, and at any time a decision is made to remove or change the classification of that document, the document shall be stamped or marked as follows:

(a) the appropriate security classification category (Top Secret, Secret, Confidential) shall be placed at the top and bottom of the front cover (if any), of each page and of the outside of the back cover (if any);

(b) the appropriate one of the following two markings shall be placed at the bottom of the first page:

SUBJECT TO GENERAL
DECLASSIFICATION SCHEDULE OF E.O. 11652
AUTOMATICALLY DOWNGRADED AT TWO YEAR
INTERVALS AND DECLASSIFIED ON

_____
(insert date or event)

or

EXEMPT FROM GENERAL
DECLASSIFICATION SCHEDULE OF E.O. 11652
EXEMPTION CATEGORY (circle one or more):
§ 5B (1), (2), (3) or (4)
AUTOMATICALLY DECLASSIFIED ON

_____
(unless impossible, insert date or event)

(c) if the document involves information or material relating to sensitive intelligence sources and methods, the following marking shall be placed at the bottom of the first page:

WARNING NOTICE —
SENSITIVE INTELLIGENCE
SOURCES AND METHODS INVOLVED

(d) if the document or material relates to communications intelligence, intelligence sources and methods or cryptography, or otherwise requires special access, distribution or protection, such additional markings as the Executive Director may prescribe shall be placed on the bottom of the first page (see also STAT).

(e) if the document contains Restricted Data, as defined in the Atomic Energy Act of 1954:

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Its dissemination or disclosure to any unauthorized person is prohibited.

(f) if the document contains Formerly Restricted Data, as defined in the Atomic Energy Act of 1954:

FORMERLY RESTRICTED DATA
Unauthorized disclsoure subject to administrative and criminal sanctions. Handle as Restricted Data in Foreign Dissemination (Atomic Energy Act of 1954, section 144. b.).

(g) if the document or material is to be furnished to persons outside the Executive Branch of the government and is not marked "Restricted Data" or "Formerly Restricted Data", the following marking shall be placed at the bottom of the first page:

NATIONAL SECURITY INFORMATION
UNAUTHORIZED DISCLOSURE SUBJECT TO CRIMINAL SANCTIONS

2. Paragraphs. Whenever a classified document contains both classified and unclassified information, or contains information of more than one security classification category, to the extent practicable each paragraph shall be marked to indicate its classification category or that it is unclassified.

3. Material Other Than Documents. The appropriate classification category shall be conspicuously marked on classified material other than documents (and on their containers, if possible). If the material or container cannot be marked, written notice of such classification shall be furnished to the holders.

DRAFT
8 June 1972

PART III. DECLASSIFYING, DOWNGRADING AND PUBLIC AVAILABILITY OF INFORMATION

A. Information Originated After June 1, 1972. Documents originating after June 1, 1972 shall be declassified and made available to the public in accordance with the following paragraphs.

1. General Declassification Schedule (GDS). Classified information originated after June 1, 1972 and not exempted from automatic declassification by action taken pursuant to paragraph 2 below shall be declassified and downgraded in accordance with the following timetable:

(a) Top Secret. Information and material originally classified Top Secret shall become automatically —

downgraded to Secret at the end of the second (2nd) full calendar year following the year in which it was originated,

downgraded to Confidential at the end of the fourth (4th) full calendar year following the year in which it was originated, and

declassified at the end of the tenth (10th) full calendar year following the year in which it was originated.

(b) Secret. Information and material originally classified Secret shall become automatically —

downgraded to Confidential at the end of the second (2nd) full calendar year following the year in which it was originated, and

declassified at the end of the eighth (8th) full calendar year following the year in which it was originated.

(c) Confidential. Information and material originally classified Confidential shall become automatically —

declassified at the end of the sixth (6th) full calendar year following the year in which it was originated.

2. Exemption from General Declassification Schedule.

(a) A Top Secret classifier shall determine that a classified document (Top Secret, Secret or Confidential) does, or does not, fall within one or more of the following exemption categories (the designations "5B(1)", "5B(2)", "5B(3)" and "5B(4)" are category designations prescribed by E.O. 11652):

5B(1). classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence;

5B(2). classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods;

5B(3). classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security;

5B(4). classified information or material the disclosure of which would place a person in immediate jeopardy.

(b) Exemption decisions required above shall take into account possible future assignments, operational relationships and cover arrangements.

(c) Documents containing Restrictive Data or Formerly Restrictive Data and so marked in accordance with Section D.1(e) or (f) of PART II are exempt from the General Declassification Schedule. No additional markings are required to accomplish such exemptions.

3. Ten (10) Year Review of Exempted Documents. Any person (including a former Presidential appointee) and any department of government, at any time after the expiration of ten (10) years from the date of origin, may request the declassification of a document

originated after June 1, 1972, which is exempt from the General Declassification Schedule. The requester shall address his request to The Assistant to the Director. The request shall be processed in accordance with the provisions of Annex A to this regulation. Any decision under the Annex to classify a document or information or to decline to declassify may be made only by an official to whom the requisite classification authority has been delegated under Section A of PART II.

4. Automatic Declassification After Thirty (30) Years.

Deputy Directors and heads of other offices which report to the Executive Director shall cause all classified documents originated after June 1, 1972 for which they have responsibility to be reviewed for declassification, prior to the time the documents become thirty (30) years old. They shall forward to the Director for his consideration and action lists which identify all such documents they believe should continue to be classified. The Director may declassify the documents, classify them at a different category of classification or continue in force their current classification category.

(a) Documents on which recommendations for continued classification are not forwarded to the Director in accordance with this paragraph and those which the Director does not continue in a classified status shall be declassified automatically at the end of the calendar year in which they become thirty (30) years old.

(b) Documents which the Director continues in a classified status under this paragraph shall be so designated on lists personally approved by the Director in writing. The list shall also specify the reasons for continued classification and the dates on which the documents shall become declassified automatically.

B. Information Originated Before June 1, 1972. Documents originated before June 1, 1972 shall be declassified and made available to the public in accordance with the following paragraphs.

1. Application of General Declassification Schedule. Documents classified under Executive Order 10501, as amended (which was superseded by E.O. 11652), or an earlier executive order, and assigned to Group 4 under E.O. 10501 are subject to the General Declassification Schedule. (See PART III. A. 1.) No other documents classified prior to June 1, 1972 shall be subject to the General Declassification Schedule.

2. Application of Ten (10) Year Review. Documents originated before June 1, 1972 and exempt from the General Declassification Schedule shall be subject to the ten (10) year review, upon the request of any person (including a former Presidential appointee) or any department of government, as prescribed by paragraph 3 of Section A of this PART.

3. Application of Automatic Declassification After Thirty (30) Years. Prior to the time they become thirty (30) years old, documents originated before June 1, 1972 and exempt from the General Declassification Schedule shall be reviewed for declassification action by the Director under the procedures prescribed by paragraph 4 of Section A of this PART. These documents do not become declassified automatically, but shall be declassified only upon review and a determination to that effect by the Director.

C. Additional Declassification Requirements. The following paragraphs apply to documents originated before or after June 1, 1972.

1. Burden of Proof. The NSC Directive provides that for the purposes of certain administrative determinations to refuse to declassify or to continue to classify, the burden of proof is on the Agency. Therefore, any decision, under the Annex to this regulation, not to declassify, or to continue to classify, shall not be made perfunctorily, but requires a deliberate, affirmative decision based on the principle prescribed for classification decisions by PART II.

2. Review and Declassification. In addition to the declassification and downgrading actions required by the preceding Sections of this PART, Agency components, to the extent practicable, shall review documents on a systematic basis and declassify and downgrade them, as warranted.

3. Authority to Declassify. Information and material may be downgraded or declassified by the official who originally classified, by his successor in capacity or by a supervisory official of either. In addition, any of the foregoing officials may authorize subordinates to downgrade and declassify.

4. Marking Downgraded or Declassified Documents. When action is taken to downgrade or declassify any document, appropriate markings (see Section D of PART II) shall be made on the document and the original markings shall be canceled. In addition, the date of the action and the authority for the action shall be indicated. When the volume of documents is such that it is impracticable to mark each document, appropriate notations may be made on the storage unit.

5. Annual Action to Make Declassified Documents Available to the Public. During each year, Deputy Directors and heads of other offices which report to the Executive Director shall take action to locate and, if practicable, segregate documents which have been determined to be of sufficient historical or other value to warrant preservation (44 U.S.C., Chapter 21) and have been or are to become declassified during the calendar year. Promptly after the beginning of the succeeding year, such officials shall make such declassified documents available to the public in accordance with the Freedom of Information Act (5 U.S.C. 552(b)) and other applicable provisions of law.

PART IV. ACCESS TO CLASSIFIED INFORMATION

Persons shall be given access to classified documents and information only in accordance with the following Sections.

A. Need-to-Know Access. Except as provided by B and C below, a person may be given access to classified information and documents only if both of the following standards are met:

1. the official having responsibility for the classified information or document must have determined that the person seeking access needs to have access in order to perform his official duties or duties based on a contract; and

2. the Director of Security must have made a determination under appropriate directives and regulations that the person is trustworthy (security clearance).

Security clearances are to be granted only for access to information of the security classification category for which access is sought. Security clearances are to be downgraded or withdrawn when the person no longer has a need to know information of that security classification category. Withdrawal or downgrading of a security clearance shall be without prejudice to the person's eligibility to be given a security clearance at a later date, should the need again arise.

B. Access By Former Presidential Appointees. Any person who previously occupied a policy-making position to which he was appointed by the President (other than a member of the White House Staff or a special committee or commission appointed by the President), may be given access by the Executive Director to classified information or material originated, reviewed, signed or received by the former official while he occupied that position, provided that:

1. the Executive Director determines that access is clearly consistent with the interests of national security; and

2. appropriate steps are taken to assure that classified information or material is not published or otherwise compromised.

C. Access By Historical Researchers. Persons outside the Executive Branch who are engaged in historical research projects may be given access to classified information upon a determination by the Executive Director that:

1. such access is clearly consistent with the interests of national security;

2. appropriate steps have been taken to assure that classified information will not be published or otherwise compromised;

3. the information or material requested is reasonably accessible and can be located and compiled with a reasonable amount of effort;

4. the historical researcher agrees to safeguard the information or material in a manner consistent with the Order and the NSC Directive; and

5. the historical researcher agrees to authorize a prior review of his notes and manuscript by the Agency for the sole purpose of determining that no classified information or material is contained therein.

An authorization for access shall be valid for the period required, but in no event longer than two (2) years. But authorizations may be renewed under the procedures prescribed above.

DRAFT
8 June 1972

PART V. DISSEMINATION, ACCOUNTABILITY AND PRODUCTION CONTROLS

A. Dissemination.

1. Consent of Originating Department to Dissemination by Recipient. Except as otherwise provided by Section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403, classified information or material originated in any department or agency and made available to CIA shall not be disseminated outside CIA without the consent of the originating department. See also [redacted] STAT

2. Dissemination of Sensitive Intelligence Information. Information or material bearing the notation "WARNING NOTICE — SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" shall not be disseminated in any manner outside authorized channels without the permission of the originating department and an assessment by the Director as to the potential risk to the national security and to the intelligence sources and methods involved. "Sensitive Intelligence" means intelligence, "the unauthorized disclosure of which could lead to counteraction (a) jeopardizing the continued productivity of intelligence sources or methods which provide intelligence vital to the national security or (b) offsetting the value of intelligence vital to the national security."

3. Classified information and documents shall be subject to such procedures as the Executive Director may prescribe to control effectively their dissemination. Particularly stringent controls shall be established to control the dissemination of Top Secret information.

B. Accountability.

1. Accountability Records. Top Secret and Secret information and material shall be subject to such accountability controls as the Executive Director may prescribe.

2. Top Secret Inventories. Procedures shall be established for the preparation and use of such inventory lists or finding aids as will facilitate accounting for Top Secret documents.

3. Top Secret Control Officers. Top Secret control officers shall be designated, as required, to receive and dispatch Top Secret documents and material and to maintain accountability records.

C. Restraints on Production of Documents.

1. Restraint on Reproduction. Documents or portions of documents containing Top Secret information shall not be reproduced without the consent of the originating office. All other classified material shall be reproduced sparingly and any stated prohibition against reproduction shall be strictly adhered to.

2. Restraint on Number of Copies. The number of copies of documents containing classified information shall be kept to a minimum to decrease the risk of compromise and to reduce storage costs.

PART VI. MANAGEMENT OF CLASSIFIED INFORMATION

A. Ensuring Compliance with E.O. 11652. The Executive Director is designated as the Agency official to take action necessary to ensure compliance with the Order, the NSC Directive and this regulation. Such actions shall include:

1. the establishment and operation of a program to familiarize all employees with the provisions of the Order, the NSC Directive and this regulation;

2. the establishment and operation of active training and orientation programs for employees concerned with classified information and material, such programs to include:

(a) briefing of new employees, and periodic reorientation of all employees, to impress upon each individual his responsibility for exercising vigilance and care in complying with the provisions of the Order, the NSC Directive and this regulation;

(b) briefing of employees at or prior to the termination of their employment or the beginning of a 60-day period of leave to remind them of the penalties provided by law for unauthorized disclosure of classified information.

B. Interagency Classification Review Committee (ICRC).

1. Establishment and Members. Section 7(A) of the Order establishes an Interagency Classification Review Committee to monitor the implementation of the Order. The Committee is composed of representatives of the Departments of State, Defense and Justice, the Atomic Energy Commission, the Central Intelligence Agency and the National Security Council staff, and a Chairman designated by the President. Representatives of other departments may be invited to participate with the Committee on matters of particular interest to those departments. Under the Directive, the Committee is to meet regularly, but not less frequently than on a monthly basis. The NSC staff representative has been appointed Executive Director of the Committee. The General Counsel of CIA has been appointed as the CIA Member of the Committee.

2. Authority and Responsibility. The Order and Directive direct the Committee to:

(a) oversee compliance with and implementation of the Order and programs established thereunder by each department and agency;

(b) take such actions as are deemed necessary to ensure uniform compliance with the Order and the Directive;

(c) establish procedures for acting on complaints and suggestions with respect to the administration of the Order, including appeals from denials of declassification requests by departmental committees (for CIA committee, see Section D of this PART);

(d) receive, consider and take action on suggestions and complaints with respect to the administration of the Order;

(e) in consultation with the department or agency concerned, ensure that appropriate action is taken on such suggestions and complaints;

(f) make a report to the head of the department or agency concerned in any case where the Interagency Classification Review Committee finds that unnecessary classification or overclassification has occurred; and

(g) seek to develop means to prevent overclassification, ensure prompt declassification, facilitate access to declassified material and eliminate unauthorized disclosure of classified information.

C. Reports and Information for Interagency Classification Review Committee. Reports and information shall be furnished the Interagency Classification Review Committee by the CIA member thereof as follows:

1. As of July 1, 1972, and quarterly thereafter, the lists of classifiers compiled by the Deputy Director for Support in accordance with paragraph 1, Section F, of this PART.

2. The reports prepared by the CIA Information Review Committee in accordance with subparagraph 2(a)(iv) of Section D of this PART.

3. The reports prepared by the Director, Central Reference Service, in accordance with Section E of this PART.

4. Such other reports, information and material as the Executive Director may order prepared, compiled or assembled in response to requests by the Chairman of the Interagency Classification Review Committee.

D. CIA Information Review Committee.

1. Establishment of Committee. A CIA Information Review Committee is established hereby, pursuant to Section 7(B)(2) of the Order, composed of the Executive Director (as Chairman), the Inspector General and the General Counsel.

2. Authority and Responsibility.

(a) Administrative Responsibilities. The Committee shall:

(i) report to the Executive Director in any case where the Committee finds that unnecessary classification or overclassification has occurred;

(ii) act on all suggestions and complaints with respect to the Agency's administration of the Order;

(iii) recommend to the Director or the Executive Director appropriate administrative action to correct abuse or violation of any provision of the Order or Directive, including notification by warning letter, formal reprimand, and, to the extent permitted by law, suspension without pay and removal;

(iv) prepare quarterly reports of Committee actions on appeals from denials of requests for classification review (see subparagraph (b) below), classification abuses and unauthorized disclosures.

(b) Appeal Authority. An Agency regulation to be published in the Federal Register in accordance with the Executive Order confers certain authority on the Committee to hear and act on appeals from Agency denials of requests to declassify information or documents. That regulation, upon its publication in the Federal Register, will be published also as Annex A to this regulation.

E. Data Index System. The Executive Director shall select categories of classified information originated in CIA which he deems as having sufficient historical or other value to warrant preservation.

The CIA member of the ICRC shall advise that Committee of these selections. Upon approval of such categories by the Interagency Classification Review Committee, the Central Reference Service, in consultation with the Directorates, shall establish a data index system for certain documents containing such information. Documents originated subsequent to December 31, 1972 shall be indexed into the system, which is to be fully operative not later than July 1, 1973. If feasible, the system shall be designed to facilitate recovery of the following data for each document indexed:

1. identity of the classifier;
2. date of classification;
3. identity of department or agency which originated the document;
4. addresses, if any;
5. subject matter;
6. category of security classification;
7. whether exempt from General Declassification Schedule;
8. applicable exemption category;
9. date set for automatic declassification;
10. event set for automatic declassification;
11. where filed.

The Director, Central Reference Service, shall recommend to the Executive Director such modifications, improvements and changes in the system as he may deem desirable, having in mind the purposes of the Executive Order and NSC Directive, the responsibilities of the Agency and cost factors. He should advise the Executive Director in this regard at least annually. With the approval of the Executive Director, he shall also prepare such reports relating to the progress and operation of the system as the Interagency Classification Review Committee may request.

F. Lists of Authorized Classifiers.

1. Titles of Positions. Each official who delegates authority to classify information under Section A of PART II shall maintain lists of the titles of the positions to which each category of security classification authority is delegated. (With respect to delegations by the Director, the actions prescribed by this Section shall be performed by the Deputy Director for Support.) He shall update these lists on a quarterly basis. He shall forward the lists, including the quarterly updatings, to the Deputy Director for Support, who shall compile Agency-wide lists for submission to the Interagency Classification Review Committee

in accordance with Section C, paragraph 1, of this PART.

2. Names of Persons Delegated Classification Authority. The Deputy Director for Support shall establish and maintain such procedures as may be necessary to enable him to furnish the names of all employees who occupied the positions to which authority to classify at each category of security classification has been delegated, and to designate the period of time in which each employee occupied each such position.

G. Identification of Classifiers. Deputy Directors and heads of other offices which report to the Executive Director shall establish such procedures as may be required to identify the person who classifies each document under the Order. If the name or title of the person who classifies a document appears on the document or on a copy thereof, no additional identification is required.

H. Loss or Possible Compromise. Any employee who has knowledge of the loss or possible compromise of classified information or documents shall immediately report the circumstances to the Director of Security. The Director of Security shall notify all interested departments and agencies in order that a damage assessment may be conducted.

If the loss or compromise occurred in CIA, the Director of Security immediately shall initiate an inquiry for the purpose of taking corrective measures and recommending appropriate administrative, disciplinary, or legal action.

I. Disciplinary Actions.

1. Prompt and stringent administrative action will be taken against any officer or employee, at any level of employment determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by or under the Order and the implementing directives. Where a violation of criminal statutes may be involved, the case will be referred promptly to the Department of Justice.

2. Any officer or employee who unnecessarily classifies or overclassifies information or material shall be notified that his actions are in violation of the Order or the implementing regulations. Repeated abuse of the classification process shall be grounds for an administrative reprimand.

3. Upon receipt of a recommendation from the CIA Information Review Committee for disciplinary action, in accordance with subparagraph 2(a)(iii) of Section D of this PART, the Director or the

Executive Director shall act promptly on the recommendation. He shall advise the Committee of the action taken on each recommendation.

J. Funding and Personnel. All components shall include in their budget submissions proposals for the request of appropriations adequate to discharge their responsibilities under this regulation. Components shall also assign personnel as may be needed to discharge such responsibilities. In both instances due regard shall be had for the mission and other responsibilities of the Agency and the component.

K. Workability of This Regulation — Recommendations. Components should monitor the administration of this regulation on a continuing basis. Any recommendations for modifications which would advance the purposes of the regulation (PART I, Section B), improve its administration, or facilitate or improve the performance of the CIA mission and responsibilities should be submitted, through command channels, to the CIA Information Review Committee.